



Financial Management Services (FMS) Performance Work Statement (PWS)

January 2016

Table of Contents

B.1	Executive Summary	5
B.2	Background	5
B.2.1	FMS Strategy	6
B.2.2	Existing Customers	6
B.3	Objectives	6
B.4	Scope	6
B.5	Task Areas	7
B.5.1	Task Area 1 – Hosting for Momentum Financials®	8
B.5.2	Task Area 2 – Operations and Maintenance for Momentum Financials®	8
B.5.3	Task Area 3 – Custom Reporting for Momentum Financials®	9
B.6	General Requirements	9
B.6.1	Project and Contract Management	10
B.6.1.1	Contract Management	10
B.6.1.2	Project Planning	11
B.6.1.3	Staffing/Resource Planning	11
B.6.1.4	Risk Management	12
B.6.1.5	Earned Value Management	12
B.6.1.6	Status Meetings	12
B.6.1.7	Other Meetings	12
B.6.1.8	Weekly Status Report	13
B.6.1.9	Monthly Status Report	13
B.6.1.10	Project Coordination	13
B.6.1.11	Configuration Management	13
B.6.1.12	Change and Release Management	15
B.6.1.13	Communications Management	16
B.6.1.14	Quality Assurance and Quality Control	16
B.6.2	Transition Services	16
B.6.2.1	Incoming Transition Management	17
B.6.2.2	Outgoing Transition Management	17
B.6.2.3	Hosting Transition and Migration Planning	17
B.6.2.4	Gap Planning and Analysis	18
B.6.2.5	Migration and Startup	18

FINANCIAL MANAGEMENT SERVICES PWS

B.6.3	Security	20
B.6.3.1	Federal IT Security Guidelines and Standards	20
B.6.3.1.1	FedRAMP Facility Requirements	21
B.6.3.2	Minimum Required IT Security Controls and Baseline Configurations.....	21
B.6.3.2.1	Security Controls	21
B.6.3.2.2	Baseline Configurations and Vulnerability Management	22
B.6.3.3	Audit Support	23
B.6.3.4	A&A Program	23
B.6.4	Federal Standards	24
B.6.4.1	Treasury Financial Manual.....	24
B.6.4.2	Common Government-wide Accounting Standards	24
C.1	Inspection and Acceptance by the Government.....	25
C.2	Responsibility for the Inspection and Acceptance.....	25
C.3	Scope of Inspection.....	25
C.4	Acceptance/Rejection by the Government.....	25
C.5	Initial Deliverables	26
C.6	Resubmitted Deliverables	26
C.7	Nonconforming Products or Services	26
D.1	Contract Clauses Incorporated by Reference.....	27
D.2	Period Of Performance	27
D.3	Place of Performance	27
D.4	Deliverables and Delivery Schedule.....	27
D.5	Delivery Instructions.....	27
D.6	Notice Regarding Late Delivery	28
E.1	Task Order Administration	30
F.1	Personnel Requirements.....	31
F.2	Facility Access	32
F.3	General Compliance Requirement	32
F.4	Interactions with Support Contractors	33
F.5	Key Personnel	34
F.6	Work Schedule.....	35
F.7	Personal Services	35
F.8	Government Furnished Supplies and Services/Property.....	35
F.9	Personnel Security Requirements	35

FINANCIAL MANAGEMENT SERVICES PWS

F.10 Data Requirements 36

F.11 Organizational Conflict of Interest 36

SECTION B - PERFORMANCE WORK STATEMENT

B.1 EXECUTIVE SUMMARY

The U.S. Department of Agriculture (USDA) Office of the Chief Financial Officer (OCFO) seeks qualified Contractors to support the Financial Management Services (FMS) offerings to new and existing customers. This support includes software, hardware, and services for Momentum Financials®. This task order is issued under the NIH Information Technology Acquisition and Assessment Center (NITAAC) government-wide acquisition contract (GWAC).

Offerors must respond to all three task areas:

- Task Area 1: Hosting for Momentum Financials®
- Task Area 2: Operations and Maintenance (O&M) for Momentum Financials®
- Task Area 3: Custom Reporting for Momentum Financials®

The Government is not obligated to exercise options with the vendor under this Task Order. The vendor is obligated to provide the hardware, software, and/or services under the terms and conditions of this Task Order.

B.2 BACKGROUND

The USDA mission is to enhance the quality of life for the American people by supporting agriculture; ensuring a safe, affordable, nutritious, and accessible food supply; caring for public lands and helping people care for private lands; supporting sound, sustainable development of rural communities; providing economic opportunities for farm and rural residents; expanding global markets for agricultural and forest products and services; and working to reduce hunger in America and throughout the world.

The OCFO for USDA is responsible for the financial leadership of the Administration. The Office of the Associate Chief Financial Officer for Financial Systems (ACFO-FS) is responsible for providing executive leadership and management vision to direct and implement corporate financial information and delegated systems to OCFO, including the management of Foundation Financial Information Systems (FFIS) and an extensive data warehouse. Also within the OCFO organization is the National Finance Center (NFC), which provides centralized, automated, and integrated systems and support services for payroll, personnel, administrative payments, accounts receivable, property management, budget, and accounting activities. Based in New Orleans, Louisiana, the NFC is an Office of Personnel Management (OPM) certified Shared Service Center.

In May 2014, the USDA OCFO was selected as a Shared Service Provider (SSP) for the Financial Management Line of Business (FMLoB) for the entire U.S. Federal government. The FMLoB was established to improve the cost, quality, and performance of financial management systems by leveraging shared service solutions to foster efficiencies in Federal financial operations. The goals of the FMLoB are to provide timely and accurate data for decision-making and facilitate stronger internal controls that ensure integrity in accounting and stewardship activities. The FMLoB also focuses on the reduction of costs by providing a competitive alternative for agencies to acquire, develop, implement, and operate financial management

SECTION B - PERFORMANCE WORK STATEMENT

systems through SSP solutions. The FMLoB is intended to provide seamless data exchange between and among Federal agencies by implementing a common language and structure for financial information and system interfaces.

B.2.1 FMS Strategy

USDA provides access to Momentum Financials® system resources as a service to other Federal agencies in partnership with the U.S. Department of the Treasury's Financial Integration and Transformation (FIT) initiative. USDA offers financial management services to Federal customers that include end-to-end financial process support, accounting support, and reporting. These services are grouped into the following three (3) categories:

- Technology Application Services
- Application Management Services
- System Implementation Services

USDA also offers the following complementary financial management services to customers:

- Platform Services
- Service Desk
- Transaction Services

B.2.2 Existing Customers

Current FMS customers include the General Services Administration (GSA) and close to 47 small clients and presidential commissions which utilize Pegasys, an instance of Momentum Financials®. The U.S. Institute of Peace is transitioning to a separate instance of Momentum Financials®. USDA plans to onboard multiple new FMS customers during the life of this Task Order.

B.3 OBJECTIVES

The purpose of this Task Order is to acquire the following for the Government:

- Continued system operations for existing FMS customers with improved system performance
- Effective enhancement support to meet changing agency needs
- Efficient on-boarding and support for new FMS customers
- Innovative industry practices that meet key performance measures
- Efficient contract and task management responsive to agency needs

B.4 SCOPE

The scope of this Task Order includes the following task areas and general requirements for Momentum Financials® which may include software, hardware, and services:

- Task Areas (see Section B.5 Task Areas)
 - Hosting
 - Operations & Maintenance (O&M)

SECTION B - PERFORMANCE WORK STATEMENT

- Custom Reporting
- General Requirements (see Section B.6 General Requirements)
 - Project and Contract Management
 - Transition Services
 - Security
 - Federal Standards

The following CIO task areas are to be used for this acquisition: 2-Chief Information Officers (CIO) Support, 4-Outsourcing, 5-IT Operations and Maintenance, 6-Integration Services, 7-Critical Infrastructure Protection and Information Assurance, 8-Digital Government, 9-Enterprise Resource Planning (ERP) and 10-Software Development. NITAAC subcontracting plans are established on the master contract (i.e. CIO-SP3) level. These plans flow down to the individual task/task order level and are not required to complete this order.

The Government intends to issue a multi-year Task Order as a result of this RFQ. The Contractor shall provide hardware, software, and/or services to accomplish the tasks of the Task Order as further described in the sections below. The work may involve utilizing USDA or FMS customer software, hardware, applications, databases, networks, and security platforms to support software, hardware, application delivery, database administration, network, security platforms configuration and integration, and any other IT professional services. At all times the service provider shall comply with existing USDA and FMS customer security standards, existing Federal guidelines and standards from NIST, and commercial best practices. The Contractor shall develop a thorough familiarization with a customer's mission and the role each system plays in the support of that mission. The Contractor shall be responsible for executing all requirements contained in the performance work statement as directed.

The government will provide the USDA owned systems to be operated under this contract, and will retain sole ownership of the financial systems.

B.5 TASK AREAS

Specific support shall be requested on an as-needed basis by the exercising of an option. Tasks shall be specifically defined in the Option Performance Work Statement (PWS) issued by the CO to the Contractor. Deliverables, reports, and time schedules shall be established within each option. Options may consist of some or all of the activities and deliverables from one or more task area. Options are not comprehensive and additional requirements within the scope of the overall Task Order may be required under the option.

Specific support addressed in this PWS includes the following task areas:

Task Area 1: Hosting for Momentum Financials®

Task Area 2: Operations and Maintenance for Momentum Financials®

Task Area 3: Custom Reporting for Momentum Financials®

SECTION B - PERFORMANCE WORK STATEMENT

B.5.1 Task Area 1 – Hosting for Momentum Financials®

The Contractor shall be responsible for providing all hardware, software, third party software licenses, and services for Momentum Financials® and related applications hosting. Hosting tasks may include data center operation; set-up and maintenance of development, testing, and production environments; hardware, software, and network maintenance and upgrades; database maintenance; performance tuning; and physical, network, and audit security. Hosting environments shall be cloud-based, Tier 3, highly available, reliable, scalable, secure, cost effective, and meet the NIST definitions of cloud services as documented in NIST SP800-145.

Activities required under this task area may include the following:

- Managed Services
 - License Management
 - Capacity Management
 - Storage Management
 - Service Level Agreement Management
 - Incident Management
 - Backup and Recovery
 - Documentation and Training
- Technical Administration
 - Database Administration
 - Server Administration
 - Network Administration
 - Maintenance Support
- Technical Optimization
- Security Support
- Audit Support

Deliverables required under this task area may include the following:

- Hardware
- Software
- System, network, security, and usage reports
- Customer Satisfaction Survey and Results
- Capacity Plans
- Incident Response Plan
- Contingency Plan/Disaster Recovery Plan
- Upgrade schedule
- COOP Plan
- Vulnerability scan results

B.5.2 Task Area 2 – Operations and Maintenance for Momentum Financials®

The Contractor shall be responsible for providing all software and services for the O&M of Momentum Financials®. O&M tasks may include ensuring that applications are free of major errors and minor errors are minimized, bug fixes, on-site support, upgrade management and execution, testing, and enhancement support.

Activities required under this task area may include the following:

- Annual Software Maintenance for Momentum Financials®
- Production Support
 - O&M for modules and interfaces
 - Service Releases
 - Batch Operations

Deliverables required under this task area may include the following:

- Batch Job reports
- Upgrade schedules
- Incident Status reports
- Customization Analysis
- Business Process Impact Analysis
- Technical Analysis

SECTION B - PERFORMANCE WORK STATEMENT

- Helpdesk Support
- Accounting Support
- Incident Management
- Support Request Management
- Development and Implementation for Minor and Major Upgrades
- Development and Implementation for New Interfaces
- Development and Implementation for New Modules
- Security Support
- Testing Support
- Database Analysis
- Training plan and materials
- Quick reference guides
- Test Strategies and Plans
- Test scripts and test results
- Assessment and Authorization (A&A) support documentation

B.5.3 Task Area 3 – Custom Reporting for Momentum Financials®

The Contractor shall be responsible for providing all software and services for Momentum Financials® custom reporting. Custom reporting tasks may include ensuring that reports meet availability and accuracy targets, modifying existing reports, developing new reports, and testing new or modified reports.

Activities required under this task area may include the following:

- Reporting O&M Support
 - Report and Query Generation
 - Report and Accounting Entry Reconciliation (e.g., subsidiary reports should reconcile to the trial balance)
 - Functional Issue Resolution
 - Maintenance of report availability, accuracy, and integrity
- Development and Implementation for Minor and Major Upgrades
- Development and Implementation for New Reports
- Testing Support
- Security Support

Deliverables required under this task area may include the following:

- Reports Conversion Analysis
- Development documentation
- Configuration documentation
- Test Strategies and Plans
- Test scripts and results
- New or modified reports

B.6 GENERAL REQUIREMENTS

The Contractor shall perform the tasks below as requested. Specific performance measures, due dates, and alterations to requirements will be stated in each option.

SECTION B - PERFORMANCE WORK STATEMENT

B.6.1 Project and Contract Management

The Contractor shall be responsible for providing all administrative and managerial resources necessary for the management of the task order. If issued multiple options, the Contractor shall make every effort to consolidate management functions and streamline project oversight. Project and Contract Management tasks may include planning, day-to-day operations and management support, quality assurance, progress/status reporting, and program reviews.

Required activities may include the following:	Required deliverables may include the following:
<ul style="list-style-type: none"> • Project Planning • Staffing/Resource Planning • Risk Management • Earned Value Management (EVM) • Coordination among multiple vendors and Government personnel • Monthly/weekly status meetings • Configuration Management • Change Management • Communications Management • Security Management • Quality Assurance and Quality Control • Documentation 	<ul style="list-style-type: none"> • Project Management Plan • Project Master Schedule • Work Plans • Work Breakdown Structures • Earned Value Management (EVM) Report • Meeting agendas and minutes • Monthly/weekly status reports

Options may exercise the project and contract management requirements described below.

B.6.1.1 Contract Management

The Contractor shall be responsible for providing all administrative and managerial resources necessary for the management of this task order. The Contractor shall:

- Develop project schedules and plans, to include deliverables in task areas
- Mobilize resources to execute the work represented in the plans
- Monitor progress against the plans
- Provide briefings and reports of activities
- Review deliverables to ensure conformance to the quality assurance plan and specifications (See B.6.1.14 Quality Assurance and Quality Control)
- Resolve support issues within its responsibility
- The Contractor shall assign personnel with substantial experience with Federal financial systems and Momentum Financials®
- Develop and execute management plans
- Serve as the primary point of contact for all project management issues and keep the Government fully informed both verbally and in writing of any concerns or problems that arise

SECTION B - PERFORMANCE WORK STATEMENT

Project Management for all development and implementation activities shall utilize the Project Management Institute (PMI) standards or equivalent. Annual Software Maintenance and O&M support shall be based on the Software Engineering Institute's (SEI's) Software Maintenance Maturity Model (SMmm or S3M) or equivalent.

Consequently, the Contractor shall establish milestones for each task against which progress shall be monitored and evaluated. These milestones must be related to distinct and measurable products. Each task shall be subdivided into discrete work elements according to a structured top-down approach that emphasizes the relationship of work elements to each other and to the overall task. The discrete work elements shall be the basis for progress reporting and for financial monitoring and control of the project.

B.6.1.2 Project Planning

Within one (1) business day of the task order award, the Contractor shall contact the COR to request a kick-off meeting. The kick-off meeting will be held at the Government site no later than ten (10) business days from the award date. The Contractor's Project Manager (Contractor PM), the key personnel, and core team shall attend the meeting. The Contractor must be prepared to discuss the following:

- A high-level management approach that addresses the scope, project assumptions, constraints, task objectives, key milestones, Contractor's project organization and Contract administration, delivery schedule, and deliverables
- A high level work plan for all O&M activities that addresses on and off-site personnel support expected by month
- A high level work plan for all development, modernization, and enhancement (DM&E) activities that addresses on and off-site personnel support expected by month
- Contractor's high-level approach and methodology to implementing planned software upgrades during the task order period of performance
- Contractor's high-level approach and methodology to any new development and implementation efforts
- Contractor's high-level approach and methodology to address risks, security, staffing/resource issues including any subcontractors
- Contractor's high-level approach and methodology to address changes, communications, and Configuration Management issues
- How the Contractor proposes to meet the EVM requirements

B.6.1.3 Staffing/Resource Planning

The Contractor shall deliver a Staffing/Resource Plan to the Government for approval (per the schedule described in the task order). The Contractor shall identify any known technology resource requirements and provide the materials that are needed to support the task order. The Contractor shall identify, secure, and utilize the minimum levels of staff, with optimal skill sets, that are required to support Momentum Financials® upon completion of a draft work plan. The Staffing/Resource Plan shall include an analysis of current and projected resource needs to meet the system requirements for performance, product quality, and security.

SECTION B - PERFORMANCE WORK STATEMENT

B.6.1.4 Risk Management

The Contractor shall deliver a Risk Management Plan to the Government for approval (per the schedule described in the task order). The objectives of the risk management plan are to identify, address, and mitigate risks before they become threats to success or major sources of rework.

The Contractor shall also be responsible for:

- Identifying appropriate mitigation strategies and solutions
- Supporting and participating in risk status reviews as directed by the COR
- Soliciting comments and guidance from the Government

B.6.1.5 Earned Value Management

For Enterprise Management Office (EMO) reportable projects, the Contractor shall develop and maintain an EVM system that is in conformance with American National Standards Institute/Electronic Industries Alliance (ANSI/EIA) Standard 748-1998. The Contractor's EVM system must be certified through an independent third party in line with ANSI/EIA Standard 748-1998 requirements regarding compliance reviews. The EVM system shall document and track project work and schedule status. Proposed revisions to the schedule must be submitted to the Government for approval via change management procedures.

The Contractor shall submit monthly EVM Reports to the Government (per the schedule described in the task order) for T&M tasks.

B.6.1.6 Status Meetings

Weekly status meetings shall be scheduled to address progress, planned activities, risks, or conflicts that may impact the schedule, scope, or cost and any change management impacts. Weekly status meetings may also include the status on the development and implementation efforts.

The Government and the Contractor PM shall jointly chair weekly status meetings and these will be attended by the Contractor and government team leads. Tasks and sub-tasks will be discussed at this meeting, with agreed upon delivery dates. The meetings shall schedule and present risks, risk status, and risk mitigation strategies.

The last weekly status meeting of the month will become a monthly status meeting where the Contractor shall discuss major schedule and project accomplishments during the month, EVM metrics, and risk mitigation strategies and efforts.

B.6.1.7 Other Meetings

The Contractor shall, if requested, attend and support Change Control Board (CCB) meetings on a weekly basis. The Contractor shall present the status of the Enterprise System for Change Management (ESC) tasks closed during the prior week, ESC tasks scheduled to be worked on the during the current week, and the following week.

SECTION B - PERFORMANCE WORK STATEMENT

In addition, ad-hoc meetings, executive briefings, and demonstrations may be requested by the Government on an as-needed basis.

The Contractor shall produce agendas at least 24 hours before scheduled meetings and meeting minutes no later than 2 business days following the meeting. The Contractor shall submit meeting agendas and minutes per the schedule described in the task order.

B.6.1.8 Weekly Status Report

In conjunction with the weekly status meetings, the Contractor shall prepare and distribute a Weekly Status Report that documents the activities and achievements in the prior week and the planned activities, milestones, deliverables due, and meetings for the following week.

B.6.1.9 Monthly Status Report

The Contractor shall prepare a Monthly Status Report, to be distributed on the last weekly status meeting of the month that documents the activities and achievements in the prior month and the planned activities, milestones, and deliverables due for the following month. The report shall document any problems or unresolved issues that may impact the triple constraint (scope, schedule, and cost).

B.6.1.10 Project Coordination

The FMS tasks involve coordination with a number of different resources which may be Government personnel or other contractors. Duties will be performed through collaboration with all parties. Proper chain of command and roles and responsibilities shall be established and maintained to work effectively in this type of environment. Coordination shall take place in writing through formal processes such as status reports and participation in project meetings and informal processes while working side by side.

The Contractor shall work effectively with the winning contractors for the following contracts:

- Helpdesk
- Independent Verification and Validation (IV&V)
- Testing Support Services
- Audit Services

B.6.1.11 Configuration Management

The Contractor shall deliver a Configuration Management Plan to the Government for approval (per the schedule described in the task order). For all development and implementation work, minor and major software upgrades, and service releases and defect/incident fixes during O&M activities, the Contractor is responsible for developing and maintaining a Configuration Management Plan in accordance with USDA's Configuration Management guidelines. The plan shall identify processes and procedures to manage and track changes once a configurable item is accepted by the Government.

SECTION B - PERFORMANCE WORK STATEMENT

The Configuration Management Plan shall be approved by the Government prior to the initiation of any configuration activities.

The Contractor shall schedule and lead configuration management meetings to address any specific defects, issues or changes submitted to the project. A configuration management meeting may determine that a change must be elevated to the CCB to approve the change and review the implications of the issue. The Contractor shall attend and support CCB meetings on a weekly basis, if requested.

Configuration Management activities also provide a logical model of the infrastructure by identifying, controlling, maintaining, and verifying installed hardware, software, and network versions. The goal is to account for all IT assets and configurations; provide accurate information on configurations; provide a sound basis for incident, problem, change, and release management; and to verify configuration records against the infrastructure and correct any exceptions.

The Contractor shall satisfy the following configuration management requirements:

- Define configuration management policies and procedures
- Establish a process for tracking configuration changes
- Use a configuration management system for tracking all deliverables
- Select, install, and maintain configuration management tools
- Enter and upload configuration data into configuration management database
- Establish process interfaces to problem management, incident management, change management, technical support, maintenance management processes, and asset management processes
- Establish appropriate authorization controls for modifying configuration items and verify compliance with software licensing
- Establish guidelines for physical and logical separation between development, test, and production, and the process for deploying and back out of configuration items
- Establish configuration baselines as reference points for rebuilds, and provide ability to revert to stable configuration states
- Establish process for verifying the accuracy of configuration items, adherence to configuration management process, and identifying process deficiencies
- Establish a configuration management repository or library that contains source codes and executable files of previous versions and current production versions
- Provide the Government with access to all processes and sub-processes in configuration management tools
- Maintain and manage off-site long-term archive backup including archive materials (tapes) transferred by the Government at transition
- Develop, deploy, and maintain near real-time interface between the Contractor's configuration/change management system and the Government's configuration/change Management System (currently using IBM ClearCase/ClearQuest) to:
 - Allow the Government to assign change requests to the Contractor and receive status reports

SECTION B - PERFORMANCE WORK STATEMENT

- Allow the Contractor to forward change requests for approval by the Government and receive approval/disapproval results

B.6.1.12 Change and Release Management

The Contractor shall deliver a Change Management Plan to the Government for approval (per the schedule described in the task order) to facilitate a workforce transition. The Change Management plan shall cover all O&M service releases and defect/incident fixes, minor and major software upgrades, new interface and module development, and implementation changes throughout the project life cycle.

Release management covers the management of software, hardware and network rollouts and the design and implementation of efficient procedures for distribution and installation of changes. Release management activities also ensure that only correct, authorized, and tested versions are installed and that changes are traceable and secure. The Contractor shall satisfy the following change management and release management requirements:

- Recommend and maintain change and release management policies, procedures, processes, and training
- Administer the version control system as it relates to release management of government applications
- Document and classify proposed changes to the government platform services
- Documentation includes cost and risk impact and back out plans of those changes and establishes release management plans for major changes
- Develop and maintain a schedule of planned changes and provide to the Government for review
- Schedule and conduct change management meetings to include review of planned changes and results of changes made. Meetings shall be conducted weekly or as required
- Update and maintain change documentation including instance parameters and system settings
- Review release management details and alter as appropriate (e.g., back out plan, go/no go decision)
- Notify the government's affected clients of changes that impact schedule, processes, tools, and services
- Implement changes and adhere to detailed release plans
- Modify configuration, asset management items, and service catalog (if applicable) to reflect changes
- Verify that any change meets objectives and resolves negative impacts
- Monitor changes and report results of changes and impacts
- Maintain master copies of new versions in a secured software library and update configuration databases
- Develop change management controls which recognize and integrate the roles of separate development, test, and production environments in the maintenance of viable applications

SECTION B - PERFORMANCE WORK STATEMENT

- Document execution and back-out plans for Government approval. Master copies of new versions shall be secured in a software library and configuration databases shall be updated

B.6.1.13 Communications Management

The Contractor shall deliver a Communications Management Plan to the Government for approval (per the schedule described in the task order). Communications among all stakeholders must be carefully managed and controlled throughout the project lifecycle. This includes communications among the Contractor, USDA, FMS customers, and the users of the system. This also includes project sponsors, stakeholders, business unit/support services, project core team members, process group owners and the COR. USDA executives shall be informed of the status of the project as it progresses and how they are impacted.

B.6.1.14 Quality Assurance and Quality Control

The Contractor shall deliver a Quality Assurance and Quality Control (QA/QC) Plan to the Government for approval (per the schedule described in the task order) and implement a QA/QC program which establishes, implements, and maintains QA/QC as it relates to technical quality for deliverables, work products, and services performed under this task order. The QA/QC program shall include management and technical reviews and audits to validate the quality of the work performed by the Contractor's personnel and of the work performed by its subcontractors. The QA/QC Program shall incorporate all processes required to develop, document, monitor, review, analyze, and conduct the Contractor's development, maintenance, and execution. It shall ensure that all developed application software and associated materials meet accepted industry standards, best practices for quality, and Federal Financial Management System requirements as detailed in OMB Circular A-127, Financial Management Systems.

The Contractor's QA/QC program shall address all requirements within the PWS and ensure adherence to the performance measures specified in the Performance Requirements Summary (PRS). The Government will use a Quality Assurance and Surveillance Plan (QASP) to measure contractor performance against the metrics defined in this PWS.

B.6.2 Transition Services

The Contractor(s) shall be responsible for providing all resources necessary for the smooth transition of work to or from other vendors related to the task order. If issued multiple options, the Contractor shall make every effort to consolidate transition functions. Transition Services tasks may include planning; training of government personnel; developing process, procedure, and system documentation; and migration activities.

Required activities may include the following:

- Transition Management
- Gap Planning and Analysis

Required deliverables may include the following:

- Transition and Migration Plan
- Implementation Plan

SECTION B - PERFORMANCE WORK STATEMENT

- Deployment Schedule
- Training plan and materials

Options may exercise the transition services requirements described below.

B.6.2.1 Incoming Transition Management

The Government will specify the number of days that the Contractor shall have to complete the transition of work from the incumbent contractor. Prior to initiation of any work, the Contractor shall submit an incoming Transition Management Plan for the anticipated phase-in work. The Contractor shall maintain the continuity and consistency of the services during the transition period without any interruption to customer operations.

B.6.2.2 Outgoing Transition Management

The Contractor shall deliver an outgoing Transition Management Plan to the Government for approval (per the schedule described in the task order) to ensure the smooth transition to a successor contractor. The Contractor shall transition the required services of the task order without interruption to the Government. The Contractor shall implement its Transition Plan upon request by the Government. However, the Government may require changes to the plan after submission. Compliance with any Government requested changes or revisions to the plan are due within 30 calendar days of the request, or sooner as negotiated.

B.6.2.3 Hosting Transition and Migration Planning

The Contractor shall develop a Transition Plan, Site Prep Plan, and Target Infrastructure Design in support of the transition of the hosting infrastructure from the existing hosting provider to the Contractor. The Transition Plan shall clearly identify and define the procurement, installation, configuration, and migration responsibilities and other dependencies for the Contractor, USDA, and other vendors. The Transition Plan shall include coordination with application managers and database administrators to ensure adequate system testing prior to cutover. In addition, the Transition Plan shall include planning for database migration, account for potential issues relating to the size of the database, identify challenges and risks, identify resources, and prevent any unplanned outages of production application or services. The Contractor shall meet the transition milestones listed in the table below.

Table B.6 Transition Milestones

Transition Milestone	Due Date
----------------------	----------

SECTION B - PERFORMANCE WORK STATEMENT

Standup of Servers and Infrastructure Complete (including establishment of network connectivity)	60 days after Date of Award
System, Load/Performance Test Complete	115 days after Date of Award
User Acceptance Test Complete	160 days after Date of Award
Release Readiness Review Complete	165 days after Date of Award
Production Cutover for Momentum	170 days after Date of Award

A project manager shall be responsible for overseeing all aspects of the approved plan. The Contractor's Project Manager shall be responsible for managing the following transition activities:

- Meeting transition milestones by completing the infrastructure preparation and helping to integrate both the USDA WAN and connect the new facility LAN to the current hosted environment
- Providing personnel to complete systems configuration and testing within the data center environment
- Meeting with USDA representatives, immediately following award, to review the transition milestones and schedule, Bills of Material (BOM), and other material required to support the Transition Plan. USDA representatives include the system owners, application and database administrators, and security officers
- Coordinating with the data center facility manager, network engineering, and other internal POCs who will play a critical role in preparing the infrastructure and providing USDA WAN and LAN connectivity, as requested by USDA
- Maintaining an action item list or issue log and developing risk mitigation strategies to prevent schedule delays
- Providing weekly status reports and meet regularly (bi-weekly minimum) with USDA management and staff to address transition schedules, issues, and action items
- Develop and implement knowledge transfer and transition procedures to ensure that government technical staff understand all components of the business and technical environment

B.6.2.3.1 Gap Planning and Analysis

In order to successfully fulfill the migration and startup requirements described below, the Contractor shall perform a thorough gap planning and analysis process, as part of the pre-migration planning activities. The outcome of this process shall be the identification and documentation of existing systems bottlenecks, dependencies, constraints and efficiencies that will be taken into consideration when designing and implementing the target infrastructure for the Momentum Financials® or related applications hosting services environment.

B.6.2.3.2 Migration and Startup

In accordance with the approach identified in Section B.6.2.3 Hosting Transition and Migration Planning above, the Contractor shall plan and execute the migration of hosted applications,

SECTION B - PERFORMANCE WORK STATEMENT

middleware components, databases, and utilities installed on or associated with each hosted server instance or image, including backup and recovery scripts and schedules from the current environment to the new cloud environment. Archive tapes from the current environment will be transferred to the control of the Contractor and migrated as necessary to maintain the ability to restore. The Contractor shall be responsible for making any changes to system and 3rd party software configuration, scripts and utilities, network, or any other item required for proper operation of Momentum Financials® or related applications in the new environment. Testing shall include the execution of load and performance test scripts via the Silk Performer tool (or an equivalent) to ensure adequate performance and to establish benchmark performance metrics for the application performance service level requirements. As required, USDA database administrators will work to keep migrated data in the new environment in sync with production data prior to final cutover.

The migrated systems and environment will be subject to a System Test and Evaluation (ST&E) and require independent Assessment and Authorization (A&A) and SAS-70 Type II certification prior to full system operations. Continuity of Operations (COOP)/Disaster Recovery procedures must be tested prior to go-live. The Contractor shall leverage common controls, policies, and procedures to the maximum extent possible in support of system A&A.

The Contractor shall support the needs of component, integration, Quality Assurance (QA) and performance testing to ensure that the implemented system meets or exceeds all requirements and specifications set forth. This includes lower level environments (development, system test and QA) availability and accessibility to USDA, its interface partners and end users.

The Contractor shall work with USDA personnel to measure the accountability and reliability of systems and components to ensure compatibility with the requirements and establish the system functional baseline. The Contractor shall work with USDA personnel on the regression testing to ensure all components are operating and performing at an acceptable level. The Contractor shall provide a responsibility matrix and assumptions around the testing effort between the contractor and Government personnel. Additionally, the Contractor shall perform integration testing and performance testing.

The Contractor shall support the continuity of essential services such as configuration management and IT security. The Contractor shall work with USDA to develop transition/support plans and provide comprehensive Go-Live support. The Contractor shall be responsible for supporting the additional computational capabilities received by USDA from external sources. Additionally, the Contractor shall:

- Replicate data to a backup facility
- Conduct a disaster recovery test
- Demonstrate business functionality at the disaster recovery site

B.6.2.3.3 Monitoring and Diagnostics

The Contractor shall provide monitoring in the cloud environments and provide USDA with reports to review environmental performance. The Contractor shall describe and provide

SECTION B - PERFORMANCE WORK STATEMENT

performance monitoring reports to USDA which include the comprehensive set of systems and associated attributes within the cloud solution (e.g., compute, memory, storage).

B.6.3 Security

The Contractor shall ensure that the system adheres to USDA IT Security Policy, Procedural/Technical Guides, and Standards. A waiver to any of these requirements must be requested and justified in writing and approved by the USDA Information System Security Manager (ISSM). The Contractor shall request these waivers and fully justify the need for each waiver in a timely manner prior to system rollout. The decision of the USDA ISSM shall be final.

- Federal Enterprise Architecture
- Privacy Act of 1974
- Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) for system accessibility requirements, <http://www.section508.gov>
- United States Department of Agriculture (USDA) Information Technology System Development Life Cycle (SDLC) Guide, Version 1.0, January 2007
- United States Department of Agriculture (USDA) Certification and Accreditation Guide, Version 4, (March 2005)
- United States Department of Agriculture (USDA) Six Step Risk Management Framework (RMF) Process Guide – Rev 2.44 May 2014
- USDA eAuthentication Guide
- “USDA Web Style Guide Version 2.0”,
http://www.fsa.usda.gov/Internet/FSA_File/usda_web_styleguide_v21111407.pdf

B.6.3.1 Federal IT Security Guidelines and Standards

The Contractor shall ensure that the software application system adheres to the following NIST Special Publications (SP) and Federal Information Processing Standards (FIPS). A waiver to any of these requirements must be requested and justified in writing and approved by the USDA ISSM.

- FIPS PUB 140-2, Security requirements for Cryptographic Modules, May 2001
- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- NIST SP 800-18 Rev. 1 - Guide for Developing Security Plans for Federal Information Systems, February 2006
- NIST SP 800-30 Rev. 1 - Risk Management Guide for Information Technology Security Risk Assessment Procedures for Information Technology Systems, September 2012
- NIST SP 800-34 Rev. 1 - Contingency Planning Guide for Information Technology and Discovery Recovery Plan, May 2010
- NIST SP 800-37 Rev. 1 - Guide for Applying the Risk Management Framework to Federal Information Systems, Feb 2010 with June 2014 Updates

SECTION B - PERFORMANCE WORK STATEMENT

- NIST SP 800-40 Rev. 3 – Guide to Enterprise Patch Management Technologies, July 2013
- NIST SP 800-41 Rev. 1 - Guidelines on Firewalls and Firewall Policy, September 2009
- NIST SP 800-44 v2 - Guidelines on Securing Public Web Servers, September 2007
- NIST 800-47 - Security Guide for Interconnecting Information Technology Systems, August 2002
- NIST SP 800-53 Rev. 4 - Recommended Security Controls for Federal Information Systems, April 2013 Updated 1/2015
- NIST SP 800-53 A Rev. 4 – Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, Dec 2014
- NIST SP 800-60 Rev. 1 - Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
- NIST SP 800-61 Rev. 2 - Computer Security Incident Handling Guide, August 2012
- NIST SP 800-64 Rev. 2 - Security Considerations in the Information System Development Life Cycle, October 2008
- NIST SP 800-77 - Guide to IPsec VPNs, December 2005
- NIST SP 800-88 - Guidelines for Media Sanitization, September 2006
- NIST SP 800-92 - Guide to Computer Security Log Management, September 2006
- NIST SP 800-95 - Guide to Secure Web Services, August 2007
- FAR 52.204-9 - Personal Identity Verification of Contractor Personnel
- NIST SP 800-53 A Rev. 4 – Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, Dec 2014, or the latest NIST SP 800-53 version when applying for a new ATO

B.6.3.1.1 FedRAMP Facility Requirements

The Contractor's hosting facilities shall be FEDRAMP certified according to the standards defined by USDA and those found at <https://fedramp.gov>. The Contractor shall maintain FedRAMP certification during the lifetime of this task order. A waiver from these requirements must be requested and justified in writing and approved by the USDA Information System Security Manager (ISSM).

B.6.3.2 Minimum Required IT Security Controls and Baseline Configurations

B.6.3.2.1 Security Controls

The Contractor shall ensure that the software applications and systems shall include all minimum IT Security controls as prescribed in NIST SP 800-53 Rev. 4 for a Moderate Baseline system. A waiver from any of these controls must be requested and justified in writing and approved by the USDA Information System Security Manager (ISSM).

Management Controls

- Certification, Accreditation, and Security Assessments (CA)
- Planning (PL)
- Risk Assessment (RA)

SECTION B - PERFORMANCE WORK STATEMENT

- System and Services Acquisition (SA)

Operational Controls

- Awareness and Training (AT)
- Configuration Management (CM)
- Contingency Planning (CP)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Personnel Security (PS)
- System and Information Integrity (SI)

Technical Controls

- Access Controls (AC)
- Audit and Accountability (AU)
- Identification and Authentication (IA)
- System and Communication Protection (SC)

Privacy Controls

- Authority and Purpose (AP)
- Accountability, Audit and Risk Management (AR)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DR)
- Individual Participation and Redress (IP)

The Contractor shall assess and evaluate minimum IT security technical controls throughout the system lifecycle including the O&M phase. The Contractor shall also assess and evaluate application related IT security management and operation controls.

B.6.3.2.2 Baseline Configurations and Vulnerability Management

The Contractor shall use Security Content Automation Protocol (SCAP) validated tools with United States Government Configuration Baseline (USGCB) or Center for Internet Security (CIS) Benchmark Scanner capability to certify that its products operate correctly with USGB or CIS Benchmark configurations. Any deviation from these baselines must be justified and requested in writing and approved by the USDA Information System Owner.

The Contractor shall use a vulnerability scanning tool to assess the system for vulnerabilities. Vulnerabilities must be reported and remediated in accordance with USDA policy. Monthly security metrics must be reportable in a format compatible and consistent with Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) reporting requirements. Requirements can be found at the following location: <https://www.us-cert.gov/cdm/home>

SECTION B - PERFORMANCE WORK STATEMENT

The Contractor shall provide access to the security management console tools to allow USDA designated personnel to view and run reports as specified in USDA policy. It is preferable to implement an integrated security reporting dashboard that provides a single point of reference for all security related reports and metrics.

B.6.3.3 Audit Support

As a Financial Shared Service Provider (FSSP), USDA is required to perform audits and reviews. These include annual Statement on Standards for Attestation Engagements (SSAE) 16 reviews, Assessment and Authorization (A&A) reviews, internal control reviews, an annual financial statement audit, an annual A-123 Review, FISMA compliance reviews, Office of the Inspector General audits, Financial Statement audits, and other possible reviews. The Contractor shall assist the Government with these audits and reviews by providing system documentation, system access, and access to their management and system personnel for interviews upon request.

Vulnerabilities or deficiencies identified during an audit review will be analyzed and mitigated in accordance with federal guidelines, auditor recommendations, and the Government's direction. In the O&M phase of the software development life cycle, the Contractor shall conduct periodic tests and internal audits of the security controls to determine that they are properly implemented, are operating as designed, and produce the expected outcomes. These tests and audits directly support USDA's own IT Security Policy by preparing the system to be audited by a third party.

Additionally, the Contractor shall provide USDA with a SSAE-16 as an assurance of the controls executed on our USDA's behalf.

B.6.3.4 A&A Program

The Contractor shall assist the Government in obtaining a successful A&A Authority to Operate (ATO) before system rollout following major software upgrades, new development, and when requested by the Government. The Contractor shall also support maintenance and recertification every three (3) years and after any major software upgrades to the system. The Contractor shall prepare the documentation required to support the A&A process in accordance with NIST 800-53 Rev. 4 - Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (or later), NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems, and other NIST guidance and USDA Policy as cited in reference documentation.

The Contractor shall support the Government's scope and planning activities, which include a preliminary Risk Assessment and System Security Plan (SSP), followed by certification preparation, ST&E resource identification, artifacts analysis, update, and acceptance during the project Initiation phase. During the Acquisition and Development phase, the Contractor shall assess security controls, assemble the certification documentation, request ATO accreditation, and distribute the A&A package. During the O&M phase, the Contractor shall perform

SECTION B - PERFORMANCE WORK STATEMENT

continuous monitoring, documentation and status reporting, reaccreditation triggers, testing training, and exercises. Should a system or component of the system be retired during the lifecycle of this contract, the Contractor shall work with the Government to see that confidential and proprietary information is properly handled.

B.6.4 Federal Standards

Federal requirements applicable to all task orders are listed below.

B.6.4.1 Treasury Financial Manual

SSP financial systems must be in accordance with the Treasury Financial Manual (TFM) (Volume I): Federal Agencies. The TFM is the Department of the Treasury's (Treasury's) official publication for financial accounting and reporting of all receipts and disbursements of the Federal Government. Treasury's Financial Management Service (FMS) issues the TFM to provide policies, procedures, and instructions for Federal departments and agencies, Federal Reserve Banks, and other concerned parties to follow in carrying out their fiscal responsibilities. Volume I of TFM applies to all Federal agencies.

Additional details on TFM Volume I can be obtained from the following location:

- <http://www.fms.treas.gov/tfm/vol1/index.html#Part%201>

B.6.4.2 Common Government-wide Accounting Standards

SSP financial systems must be maintained in accordance with the Common Government-wide Accounting Classification (CGAC) Structure. CGAC is a FMLoB initiative taken up by the Office of Management and Budget (OMB) to assist agencies with their financial management system modernization efforts, and to reduce the cost and risk of implementing and maintaining these systems.

The CGAC structure establishes a standard method for classifying the financial effects of government business activities. Although a number of standards exist for classifying financial transactions, the CGAC standards provide latitude for each agency to develop its own classification structure. As a result, the classification structures used in agency systems vary from agency to agency and often from bureau to bureau within the same agency.

The CGAC structure increases standardization in the following ways:

- Identifies the elements to be used for classification
- Establishes standard names, definitions, and formats for the elements
- Aligns the values of similar codes used by OMB and Treasury

Additional information on CGAC is provided by the Treasury's Office of Financial Innovation and Transformation ("FIT") group.

SECTION C – INSPECTION AND ACCEPTANCE

C.1 INSPECTION AND ACCEPTANCE BY THE GOVERNMENT

The Government will review and verify that all deliverables associated with the Contract and task orders fulfill the requirements and standards stated therein.

The Contractor's performance and all submitted deliverables will be evaluated for conformance with the performance requirements set forth in the task orders. Reports, documents, and narrative-type deliverables will be accepted when all Government comments/revisions, when applicable, have been incorporated.

C.2 RESPONSIBILITY FOR THE INSPECTION AND ACCEPTANCE

The Government, through its authorized representative, the COR, as specified in Section E and each task order, has the right, at all reasonable times, to inspect, or otherwise evaluate the work performed, or being performed, hereunder and shall notify the Contractor of unsatisfactory performance. All inspections and evaluations shall be performed in such a manner as will not unduly delay the work.

It will be the responsibility of the COR to ensure that adequate records of the inspection or evaluation are kept to support acceptance or rejection of work performed or being performed. Acceptance will be made by the COR or designated representative(s); rejections, if necessary, will be made by the CO.

C.3 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to the requirements (including any applicable standards), as specified in the task order. Inspection will include validation of information by the COR. The scope and nature of inspection will be determined by the COR and will be sufficiently comprehensive to ensure the completeness, quality, timeliness and adequacy of all deliverables.

C.4 ACCEPTANCE/REJECTION BY THE GOVERNMENT

The Government will provide written notification of acceptance or rejection of all deliverables within 10 business days for the draft deliverable and five (5) business days for the final deliverable. All notifications of rejection will issued by the CO and will be accompanied by specific reason(s) for rejection.

If the Government fails to complete the review within 10 business days after receiving the draft form, the deliverable will become acceptable on an interim basis for payment only. If deficiencies are discovered after this period, the Government will provide in writing a description of all discrepancies to be corrected by the Contractor. After receiving the discrepancies, the Contractor shall incorporate the changes into the deliverable and resubmit the deliverable to the Government within 10 business days.

SECTION C – INSPECTION AND ACCEPTANCE

C.5 INITIAL DELIVERABLES

Inspection and acceptance of initial deliverables procedures are as follows:

- a. The Government will provide acceptance, comments, and/or change requests, if any, within 10 business days from receipt by the Government, of all required deliverables
- b. Upon receipt of the Government comments, the Contractor shall have five (5) business days to rectify the situation and re-submit the deliverable(s) if it is not a “draft” deliverable. If it is a “draft” deliverable, the Contractor shall rectify the situation before the next scheduled submission of the deliverable(s)

C.6 RESUBMITTED DELIVERABLES

The Government will review and verify that the original problem(s) has (have) been resolved with the deliverable(s) as re-submitted. If this is a re-submission of a final deliverable, the Government will provide the Contractor written notice of acceptance/rejection or request for extension within five (5) business days after receipt of each re-submitted final deliverable.

C.7 NONCONFORMING PRODUCTS OR SERVICES

Nonconforming products or services may be rejected. Deficiencies shall be corrected within 30 business days of the rejection notice. If the deficiencies cannot be corrected within 30 business days, the Contractor shall immediately notify the CO of the reason for the delay and provide a proposed corrective action plan within 10 business days.

The Contractor’s quality control records shall identify, as part of the performance record of the task orders, the following:

- a. The number and types of deficiencies found
- b. Decisions regarding the acceptability of processes, products, and corrective action procedures

[End of Section]

SECTION D – DELIVERABLES / PERFORMANCE

D.1 CONTRACT CLAUSES INCORPORATED BY REFERENCE

- See Article F.3 Clauses Incorporated by Reference, FAR 52.252-2 (February 1998) of the CIO-SP3 Contract (Conformed) October 2015

D.2 PERIOD OF PERFORMANCE

The period of performance for the FMS Task Order shall begin on the award date and extend for 10 years. The target award date is the fourth quarter of FY 2016.

The Base period will be from August 1, 2016 – September 30, 2016 with nine (9) 1-year option periods and one (1) nine month option period. Exercising of the option periods is dependent upon continuing need of the software and service and the availability of funding.

Year	Duration	Target Dates (Calendar)
Base Period	3 Months	August 1, 2016 – September 30, 2016
Option Period 1	12 Months	October 1, 2016 – September 30, 2017
Option Period 2	12 Months	October 1, 2017 – September 30, 2018
Option Period 3	12 Months	October 1, 2018 – September 30, 2019
Option Period 4	12 Months	October 1, 2019 – September 30, 2020
Option Period 5	12 Months	October 1, 2020 – September 30, 2021
Option Period 6	12 Months	October 1, 2021 – September 30, 2022
Option Period 7	12 Months	October 1, 2022 – September 30, 2023
Option Period 8	12 Months	October 1, 2023 – September 30, 2024
Option Period 9	12 Months	October 1, 2024 – September 30, 2025
Option Period 10	9 Months	October 1, 2025 – July 31, 2026

D.3 PLACE OF PERFORMANCE

Options will specify the place of performance although the majority of the work will be performed at the contractor location. Quarterly Program Reviews will take place in the Washington, D.C. metropolitan area or through teleconference. Local travel is defined as travel within a 50-mile radius of place of performance. Local Travel will not be reimbursed. Telework arrangements for individual options may be approved by the COR.

D.4 DELIVERABLES AND DELIVERY SCHEDULE

The Contractor shall prepare and deliver the task deliverables per schedule and acceptance criteria listed in Table D.1. Individual task orders will specify additional deliverable and delivery schedule criteria.

D.5 DELIVERY INSTRUCTIONS

All task order deliverables shall be delivered to the COR no later than Noon on the date specified in the delivery schedule or as agreed to by the COR unless otherwise specified in the option.

SECTION D – DELIVERABLES / PERFORMANCE

Deliverables are to be transmitted with a cover letter, on the prime Contractor's letterhead, describing the contents. All deliverables should be delivered in electronic form in Microsoft Office formats such as Word, Excel, PowerPoint, and Project. The Government may request that deliverables are delivered in hard copy as well. Code and deployed software shall be delivered in a format that is acceptable to the Government and shall conform to an approved Configuration Management process.

Electronic copies of all task order deliverables shall be submitted to the COR at the following email address:

COR:

- Kevin Gerken
Kevin.Gerken@nfc.usda.gov

Deliverables for each task order will be delivered to the COR assigned to that task order.

D.6 NOTICE REGARDING LATE DELIVERY

In the event the Contractor anticipates difficulty in complying with any delivery dates, the Contractor shall immediately notify the appropriate COR in writing, giving pertinent details, including the date on which delivery is expected. This data shall be informational in nature and receipt thereof shall not be construed as a waiver by the Government of any schedule, rights, or remedy.

SECTION D – DELIVERABLES / PERFORMANCE**Table D.1 – Deliverables and Acceptance Criteria**

#	TASK	DELIVERABLE	DUE DATE / FREQUENCY	GOVERNMENT ACCEPTANCE CRITERIA	VENDOR PROPOSED ACCEPTANCE CRITERIA
1.	B.7.4	Quarterly Program Review	<ul style="list-style-type: none"> Quarterly, beginning with award of first task order 	<ul style="list-style-type: none"> TBD 	<ul style="list-style-type: none">

[End of Section]

SECTION E – CONTRACT ADMINISTRATION DATA

E.1 TASK ORDER ADMINISTRATION

A COR has been appointed and is responsible for all Task Order functions including budgeting, administration, task in-scope technical direction, and task results.

COR:

- Kevin Gerken
Kevin.Gerken@nfc.usda.gov

[End of Section]

SECTION F – SPECIAL CONTRACT REQUIREMENTS

F.1 PERSONNEL REQUIREMENTS

The Contractor personnel shall have knowledge and successful experience in supporting task order requirements including but not limited to the following:

- Momentum Financials®
- O&M (production support)
- Minor and major software upgrades
- Development and implementation of new interfaces
- Development and implementation of new modules
- Annual software maintenance for Momentum Financials®
- Accounting and technical support
- Tivoli
- Operations and maintenance for reports
- Development and implementation of new reports
- Extract, Transform, and Load (ETL) tools
- Extensive knowledge and experience with data center hosting, migration, management, and project execution
- Hands-on experience and vendor certified operations and system engineering expertise on the following Server Operating System platforms: Windows 2008 Server, AIX 6.x and Red Hat Linux Enterprise Server 6.x or later versions. Ability to install, troubleshoot, and configure security and hardening of the above specified operating systems
- General IT work experience in architecture, process engineering, software development and deployment, system integration, Web application delivery, and application operations
- Knowledge and experience with information management, gathering, and reporting. Ability to present analytical reports, graphs, and presentations related to loads and performance of operational Web sites, applications, databases, and network capacities
- Significant IT project planning, management, and reporting experience. Prior experience in managing large multi-agency federal government/multiple private organization IT projects is required
- Extensive knowledge and experience with project management methodologies and industry best practices. Ability to prepare project management plans, coordinate agreements, track actual performance and cost against planned, prepare summary reports, and close projects/tasks
- Extensive knowledge and experience with network architecture development and deployment methodologies to assure capacity, reliability, redundancy, failover, scalability, and local and multi-site load balancing architecture
- Extensive knowledge and experience with network security and infrastructure implementation and management. Ability to monitor network activities and detect network traffic pattern in real time setting
- Network engineering certification for configuring, monitoring, and managing network infrastructure. Ability to administer, monitor, install, configure, patch, upgrade, and troubleshoot network components

SECTION F – SPECIAL CONTRACT REQUIREMENTS

- IT security certification for perimeter, network, and application security implementation, administration, and monitoring. Ability to install, configure, manage, patch, upgrade, and troubleshoot security components
- Oracle Certified Professional (OCP) Certification for the most current Oracle database architecture and components. Ability to administer, tune, monitor, install, configure, manage, patch, upgrade, backup, and restore architecture/components
- Knowledge of Business Objects and Business Intelligence Reporting Tool (BIRT) business intelligence software
- Knowledge and experience with Microsoft Active Directory (AD) and Light Directory Access Protocol (LDAP) architectures and their roles in an integrated environment. Ability to configure Oracle and Linux LDAP services to utilize AD authentication
- Experience administering and supporting 3rd-party software and middleware components
- Knowledge and experience to tune 3rd-party software and middleware component configurations to achieve and maintain adequate performance and proper operation of the Momentum Financials® application
- Knowledge and experience to implement 3rd-party software and middleware configurations to support the Momentum Financials® application per installation guides
- Knowledge and experience to deploy Momentum Financials® application components into test and production environments

The key staff assigned to task orders shall be able to demonstrate their experience to fulfill tasks identified in the PWS. The personnel must have the required skills and domain expertise to support the requirements in the PWS.

F.2 FACILITY ACCESS

The COR will advise the Contractor regarding procedures for means of access to Government premises, delivery and storage of materials, use of approaches, corridors, elevators, and similar matters. While in the Government facility, all Contractor personnel shall be required to wear a Building Access Pass in a manner that can be seen at all times. It is the Contractor's responsibility to return passes to the COR or designee when a Contractor employee is dismissed, terminated, or assigned to duties not within the scope of this task order. The Contractor shall notify the COR when an employee's building pass is lost, and shall apply immediately for a replacement pass.

F.3 GENERAL COMPLIANCE REQUIREMENT

All deliverables and work products resulting from the task order are the property of the Government. The Contractor shall be responsible for adhering to all aspects of the Privacy Act and is prohibited from removing from the work site any programs, documentation, or data without the knowledge and written approval of the COR.

AGAR 452.224-70 Confidentiality of Information (FEB 1988)

SECTION F – SPECIAL CONTRACT REQUIREMENTS

(a) Confidential information, as used in this clause, means -- (1) information or data of a personal nature, proprietary about an individual, or (2) information or data submitted by or pertaining to an organization.

(b) In addition to the types of confidential information described in (a)(1) and (2) above, information which might require special consideration with regard to the timing of its disclosure may derive from studies or research, during which public disclosure of primarily invalidated findings could create an erroneous conclusion which might threaten public health or safety if acted upon.

(c) The Contracting Officer and the Contractor may, by mutual consent, identify elsewhere in this contract specific information and/or categories of information which the Government will furnish to the Contractor or that the Contractor is expected to generate which is confidential. Similarly, the contracting Officer and the Contractor may, by mutual consent, identify such confidential information from time to time during the performance of the task order. Failure to agree will be settled pursuant to the "Disputes" clause.

(d) If it is established that information to be utilized under this task order is subject to the Privacy Act, the Contractor will follow the rules and procedures of disclosure set forth in the Privacy Act of 1974, 5 U.S.C. 552a, and implementing regulations and policies, with respect to systems of records determined to be subject to the Privacy Act.

(e) Confidential information, as defined in (a)(1) and (2) above, shall not be disclosed without the prior written consent of the individual, institution or organization.

(f) Written advance notice of at least 45 days will be provided to the Contracting Officer of the Contractor's intent to release findings of studies or research, which have the possibility of adverse effects on the public or the Federal agency, as described in (b) above. If the Contracting Officer does not pose any objections in writing within the 45 day period, the contractor may proceed with disclosure. Disagreements not resolved by the Contractor and Contracting Officer will be settled pursuant to the "Disputes" clause.

(g) Whenever the Contractor is uncertain with regard to the proper handling of material under the task order, or if the material in question is subject to the Privacy Act or is confidential information subject to the provisions of this clause, the Contractor shall obtain a written determination from the Contracting Officer prior to any release, disclosure, dissemination, or publication.

(h) The provisions of paragraph (e) of this clause shall not apply when the information is subject to conflicting or overlapping provisions in other Federal, State or local laws.

(End of Clause)

The task order work shall be manned to the level specified in the quote throughout the work effort. Once the task order has been awarded, any changes in the staffing levels originally proposed by the vendor shall be submitted to the CO for approval. Upon approval, a modification to the task order will be awarded.

F.4 INTERACTIONS WITH SUPPORT CONTRACTORS

The Contractor shall be required to interact with the USDA or FMS customer support contractors including the Government's IV&V contractor, Testing Support contractor, Helpdesk contractor,

SECTION F – SPECIAL CONTRACT REQUIREMENTS

Audit services contractor, and any other USDA or customer contractors who are supporting the systems interfaced by Momentum Financials®.

F.5 KEY PERSONNEL

The Contractor shall assign qualified personnel to manage the task order and provide a single point of contact for management of the task order. Certain individuals shall be designated as Key Personnel who have unique qualifications identified in each task order. Key Personnel shall be dedicated and full time. Key Personnel must be experts in their field. Key Personnel shall not be replaced without prior approval from the COR.

The Contractor shall notify the CO, in writing, of a proposed substitution of key personnel. This notification shall be submitted at least 15 calendar days in advance of the proposed substitution. All proposed substitutes should have qualifications equal to, or greater than, the person to be replaced.

Certain skilled and experienced professional and technical personnel are essential for the Government to accomplish the work to be performed under this task order. Key personnel will be monitored using the following:

- At the time of task order award, the Contractor shall indicate the names and positions and provide resumes of the key personnel that will be assigned to the task order, if different from those submitted for evaluation of the quote
- For the duration of the task order, substitutions shall be made of accepted key personnel per this subsection. If one (1) or more of the key personnel becomes, or is expected to become, unavailable for work for any of the stated reasons, the task order may be amended according to the procedures as outlined in this subsection
- During the first ninety (90) days of performance, the Contractor shall make no substitutions of key personnel unless the substitution is necessitated by illness, death, or termination of employment. The Contractor shall notify the Contracting Officer within 15 calendar days after the occurrence of any of these events
- All notifications for approval of substitutions of personnel shall be submitted in writing to the CO at least 15 calendar days in advance of the effective date. The request shall provide a detailed explanation of the circumstances causing the proposed substitution, a complete resume for the proposed substitute and any other information requested by the CO. All proposed substitutions shall be determined by the Government to have qualifications, experience, and job status at least equivalent to the person being replaced or consideration shall be granted to the Government and any applicable task order price or fixed fee may be equitably adjusted downward to compensate the Government
- If it is determined that suitable and timely replacement of key personnel who have been terminated or have become unavailable for work is not forthcoming or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the task order, the task order may be terminated for default
- If the key personnel's performance is deemed unsatisfactory, the Government reserves the right to request, by written notification, and receive satisfactory personnel replacement at no additional cost within 15 calendar days of issuance of the written notification of the

SECTION F – SPECIAL CONTRACT REQUIREMENTS

unsatisfactory performance from the CO. This notification shall explain the basis for the unsatisfactory performance

F.6 WORK SCHEDULE

The Contractor may choose an appropriate work schedule. However, the Contractor shall ensure that key personnel will be available during core customer hours (8:30 AM-4:30 PM) Monday through Friday, except Federal Government Holidays and attend meetings requested/scheduled by the Government as and when required to discuss relevant project issues and progress. Options may require different core customer hours than those stated above. Certain staff shall be required to provide around the clock coverage, 24x7x365, in physical facilities, network management, security monitoring, and application support.

F.7 PERSONAL SERVICES

The Government has determined that use of a NITAAC GWAC to satisfy this requirement is in the best interest of the Government, economic and other factors considered, and this task order is not being used to procure personal services prohibited by the Federal Acquisition Regulation (FAR) Part 37.104 titled “Personal Services Contract.”

F.8 GOVERNMENT FURNISHED SUPPLIES AND SERVICES/PROPERTY

Government furnished supplies and services shall be used in conjunction with requirements under this task order and for no other purpose. Misuse of Government supplies and services may be grounds for task order termination and criminal prosecution. Government furnished supplies and services will be listed as appropriate in the Options.

F.9 PERSONNEL SECURITY REQUIREMENTS

The Contractor shall adhere to all security-related laws, requirements, and regulations that bind the Government. The Contractor shall have all new staff members complete a confidentiality agreement prior to employment. The contractor personnel involved in the management, operation, programming, maintenance, and/or use of information technology shall be aware of these responsibilities and fulfill them.

Background investigations and fingerprinting are required for all government and contractor employees. If the Government receives an unsuitable report of any contractor employee after review and processing of security background information, the Contractor will be advised immediately and such employee shall not continue to support USDA or be assigned work under this or any USDA contract. The Contractor shall replace such employee with a new employee within 30 calendar days. The minimum Personnel Security Investigative (PSI) requirement for a Contractor is a National Agency Check with Inquiries (NACI). All positions within USDA are assigned Position Sensitivity Designations (PSDs) based upon the risk/damage an unauthorized disclosure would cause to the Agency and/or National Security. The COR will advise the Contractor of the assigned designation and investigative requirements at the kickoff meeting/at the onset of task order discussions. Based upon the assigned sensitivity designation, the

SECTION F – SPECIAL CONTRACT REQUIREMENTS

minimum level PSI may not meet the requirements and a higher level of investigation and/or Security Clearance may be required.

F.10 DATA REQUIREMENTS

All files, records, papers, or machine-readable materials created or revised using equipment or material provided under this task order, are the property of the United States. The Contractor shall not replicate or reproduce information unless specifically approved in writing by the CO. The Contractor shall adhere to all rules, regulations, and procedures relating to security and confidentiality for work performed and any information handled in the course of this work.

If Contractor-furnished equipment and material is used, the Contractor shall be responsible for ensuring that only commercial, duly licensed software is used. Under no circumstances may “bootleg”, “pirated,” or other unofficial copies of software be installed on equipment. Within one (1) business day of any written request from the CO, the Contractor shall furnish proof of legitimate purchase, or license, of the software use.

F.11 ORGANIZATIONAL CONFLICT OF INTEREST

The Offeror is hereby advised that organizational conflict of interest considerations demand that the awardee of this task order will be prohibited from bidding or accepting award of any contract, subcontract, or task that requires the development of specifications or statements of work for tasks such as those described herein. The Offeror’s attention is directed to FAR Subpart 9.5, Organizational Conflicts of Interest.

[End of Section]